

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007194

International filing date: 07 April 2005 (07.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-118807
Filing date: 14 April 2004 (14.04.2004)

Date of receipt at the International Bureau: 20 May 2005 (20.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2004年 4月14日

出 願 番 号
Application Number: 特願2004-118807

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

J P 2004-118807

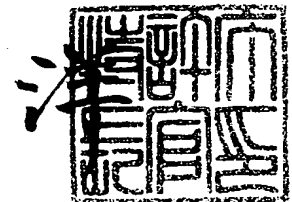
The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

出 願 人
Applicant(s): 松下電器産業株式会社

2005年 4月27日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2968260003
【あて先】 特許庁長官 殿
【国際特許分類】 G06K 19/00
【発明者】
 【住所又は居所】 広島県東広島市鏡山3丁目10番18号 株式会社松下電器情報
 システム広島研究所内
 【氏名】 中部 太志
【発明者】
 【住所又は居所】 広島県東広島市鏡山3丁目10番18号 株式会社松下電器情報
 システム広島研究所内
 【氏名】 植田 栄治
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100105175
 【弁理士】
 【氏名又は名称】 山広 宗則
 【電話番号】 082-222-9109
【選任した代理人】
 【識別番号】 100105197
 【弁理士】
 【氏名又は名称】 岩本 牧子
【手数料の表示】
 【予納台帳番号】 043775
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 02150.6

【書類名】特許請求の範囲

【請求項 1】

リーダライタと所定の方式により非接触通信を行う、非接触 IC カードにおいて、
乱数によりカード ID を生成する乱数カード ID 生成手段と、
乱数カード ID 生成手段により生成されたカード ID を記憶するカード ID 記憶手段と

カード ID 読み出しが初回か否かを判定する初回判定手段と、

カード ID の読み出し処理を行うカード ID 読み出し手段とを備え、

前記非接触 IC カードは、電源投入後、前記リーダライタから初めてカード ID の読み出し要求を受けた場合、前記乱数カード ID 生成手段によりカード ID を生成し、該カード ID をリーダライタに通知するとともに、該カード ID を前記カード ID 記憶手段に記憶し、

電源投入後 2 回目以降に、前記リーダライタからカード ID の読み出し要求を受けた場合、前記カード ID 記憶手段に記憶されたカード ID を読み出し該カード ID をリーダライタに通知することを特徴とする非接触 IC カード。

【請求項 2】

前記非接触 IC カードはさらに、リーダライタとの通信の終了を判定する、通信終了判定手段を具備し、

前記通信終了判定手段がリーダライタとの通信の終了を判定した場合、前記乱数カード ID 生成手段によりカード ID を生成し、該カード ID を、カード ID 記憶手段に記憶することを特徴とする請求項 1 記載の非接触 IC カード。

【請求項 3】

前記乱数カード ID 生成手段は、固定値部分と乱数部分で構成されるカード ID を生成することを特徴とする請求項 1 記載の非接触 IC カード。

【請求項 4】

前記非接触 IC カードはさらに、非接触 IC カードの動作条件を示す動作モードを判定するモード判定手段と、

固定のカード ID を生成する固定カード ID 生成手段を備え、

前記非接触 IC カードは、電源投入後、前記リーダライタから初めてカード ID の読み出し要求を受けた場合、前記モード判定手段によるモード判定に基づき、前記乱数カード ID 生成手段または、前記固定カード ID 生成手段を用いてカード ID を生成することを特徴とする請求項 1 記載の非接触 IC カード。

【請求項 5】

前記非接触 IC カードはさらに、前記動作モードは、検査工程での動作であることを示すハードウェア検査モードと、一般ユーザが使用する環境での動作であることを示す運用モードを含み、

前記ハードウェア検査モードでは、前記固定カード ID 生成手段を用いてカード ID の生成を行い、

前記運用モードでは、前記乱数カード ID 生成手段を用いてカード ID の生成を行うことを特徴とする請求項 4 記載の非接触 IC カード。

【請求項 6】

前記固定カード ID 生成手段は、書換え不可な ROM (リードオンリーメモリ) に記載された内容に基づき、カード ID を生成することを特徴とする請求項 4 記載の非接触 IC カード。

【請求項 7】

前記固定カード ID 生成手段は、書換え可能な不揮発メモリに記載された内容に基づき、カード ID を生成することを特徴とする請求項 4 記載の非接触 IC カード。

【請求項 8】

前記書換え可能な不揮発メモリは、EEPROM (Electrically Erasable Programmable Read Only Memory)、FeR

AM (Ferroelectric Random Access Memory)、M
RAM (Magnetoresistive Random Access Memory)、OUM (Ovonic Unified memory) のいずれかであることを
特徴とする請求項4記載の非接触ICカード。

【請求項9】

前記リーダライタと前記非接触ICカード間の通信方式はISO/IEC14443で
あり、カードIDは、前記リーダライタから前記非接触ICカードに対する初期要求リク
エストに対応したレスポンスにおけるPUP1 (Pseudo-Unique PICC
Identifier) として設定されることを特徴とする請求項1記載の非接触IC
カード。

【請求項10】

リーダライタと所定の方式により非接触通信を行う、非接触ICカードにおいて、該カ
ードに備えるCPUにより実行される制御プログラムであって、

前記非接触ICカードは、電源投入後、前記リーダライタから初めてカードIDの読み
出し要求を受けた場合、乱数によりカードIDを生成し、該カードIDをリーダライタに
通知するとともに、

該カードIDを記憶し、電源投入後2回目以降に、前記リーダライタからカードIDの
読み出し要求を受けた場合、記憶されたカードIDを読み出し、該カードIDをリーダ
ライタに通知することを特徴とするカードID生成プログラム。

【請求項11】

リーダライタと所定の方式により非接触通信を行う、非接触ICカードのカードID生
成集積回路であって、

乱数によりカードIDを生成する乱数カードID生成手段と、

乱数カードID生成手段により生成されたカードIDを記憶するカードID記憶手段と

カードID読み出しが初回か否かを判定する初回判定手段と、

カードIDの読み出し処理を行うカードID読み出し手段とを備え、

電源投入後、前記リーダライタから初めてカードIDの読み出し要求を受けた場合、前
記乱数カードID生成手段によりカードIDを生成し、該カードIDを出力することで、
リーダライタに通知するとともに、該カードIDを前記カードID記憶手段に記憶し、

電源投入後2回目以降に、前記リーダライタからカードIDの読み出し要求を受けた場
合、前記カードID記憶手段に記憶されたカードIDを読み出し、該カードIDを出力す
ることで、リーダライタに通知することを特徴とする非接触ICカードのカードID生成
集積回路。

【書類名】明細書

【発明の名称】非接触ＩＣカード、カードＩＤ生成プログラム、及び非接触ＩＣカードのカードＩＤ生成集積回路

【技術分野】

【０００１】

本発明は非接触ＩＣカードのカード識別のためのカードＩＤの生成方法及び生成手段に関するものである。

【背景技術】

【０００２】

従来、電磁誘導方式等を用いてデータの授受を行う非接触ＩＣカードと当該非接触ＩＣカードを認識するリーダライタとの間の通信には、スロット方式を採用している。これは、複数の非接触ＩＣカードが同時にリーダライタの通信エリア内に存在し、リーダライタからのポーリングに対して複数の非接触ＩＣカードが同時に応答信号を送信した場合、各応答信号が衝突して何れの非接触ＩＣカードもリーダライタと正常に通信することができなくなるためである。

【０００３】

タイムスロット方式の通信を以下に説明する。

(１) リーダライタは非接触ＩＣカードの存在を確認するため初期要求リクエストコマンドを非接触ＩＣカードへ送信する。初期要求リクエストコマンドには、非接触ＩＣカードが初期応答可能な「スロット数」が含まれる。

(２) 非接触ＩＣカードは初期要求リクエストコマンドを受信後、特定時間から開始されるタイムスロット（１～「スロット数」）へ初期応答を返す。応答するスロットは、非接触ＩＣカード自身で決定する。

(３) リーダライタは非接触ＩＣカードからの初期応答の衝突を検出した場合、再度初期要求リクエストを非接触ＩＣカードへ送信し、タイムスロットを新規に再開する。

(４) リーダライタはすべてのスロットにおいて、非接触ＩＣカードからの初期応答の衝突を検出できなかった場合、すべての非接触ＩＣカードの認識をすることができ、カード識別のシーケンスを完了する。

【０００４】

また、応答するタイミングをリーダライタが通知するスロットマーカ方式も存在するが、ＩＣカードが乱数で応答するスロットを決定する方法は同じである。ここで、各非接触ＩＣカードをリーダライタが識別するためには、各非接触ＩＣカードが異なる識別用のカードＩＤを持つ必要がある。リーダライタは、異なる識別用のカードＩＤを使用して通信する非接触ＩＣカードを特定する。このような通信の方式としては、国際規格ＩＳＯ／ＩＥＣ 14443 Type Bで規格化されている。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、前記従来の構成において、非接触ＩＣカードのカードＩＤについて、特定の値をＲＯＭ(Read Only Memory)に搭載し、その値をカードＩＤとして応答する非接触ＩＣカードの場合、非接触ＩＣカードが応答するカードＩＤが個人を特定するＩＤとなり、個人のプライバシーを侵害する可能性がある。

これは、リーダライタから送信される初期要求リクエストコマンドに対して、非接触ＩＣカードはカードＩＤを含む初期応答を返す必要があり、例えば、初期応答を異なる場所の複数のリーダライタで記録し、その記録を解析することにより、個人の行動範囲や、行動時間の特定が出来てしまうからである。

また、このような問題に対応するために、リーダライタから送信される初期要求リクエストコマンドを受け取ったＩＣカードは、初期要求リクエスト毎にカードＩＤを変更して、初期応答を行うことが考えられるが、初期要求リクエストコマンド毎に、非接触ＩＣカードのカードＩＤが変更されるため、リーダライタが特定のカードＩＤの非接触ＩＣカー

ドとの通信を行うことが出来なくなる。

【0006】

本発明は、前記従来の課題を解決するもので、個人のプライバシー保護を実現し、また、さらに、リーダーライターが特定のカードIDの非接触ICカードとの通信が可能よう非接触ICカードにおけるカードID生成方法を提供することを目的とする。

【課題を解決するための手段】

【0007】

前記従来の課題を解決するために、本発明の非接触ICカードは、乱数によりカードIDを生成する乱数カードID生成手段、乱数カードID生成手段により生成されたカードIDを記憶するカードID記憶手段、カードID読み出しが初回か否かを判定する初回判定手段、及び、カードIDの読み出し処理を行うカードID読み出し手段を備え、電源投入後初めての処理の場合、乱数カードID生成手段によりカードIDを生成し、これを利用し、2回目以後の場合、カードID記憶手段に記憶されたカードIDを使用するように構成した。

【0008】

また、本発明の非接触ICカードは、さらに通信の終了判定手段を備え、通信終了判定手段が通信の終了と判定した場合、再度乱数カードID生成手段によりカードIDを生成するように構成した。

【0009】

また、本発明の非接触ICカードにおいて生成されるカードIDは固定値部分と乱数部分で構成されている。

【0010】

また、本発明の非接触ICカードは、複数の動作モードを有し、動作モードを判定するモード判定手段、固定のカードIDを生成する固定カードID生成手段を備え、カードID読み出し処理は、モード判定手段により判定されるモードに基づき、電源投入後初めてのカードID読み出しの場合、乱数カードID生成手段または、固定カードID生成手段を用いてカードIDを生成するように構成した。

【0011】

また、本発明の非接触ICカードは、ハードウェア検査モードと運用モードの2つのモードを持ち、ハードウェア検査モードでは固定カードID生成手段を用い、運用モードでは乱数カードID生成手段を用いるように構成した。

【0012】

また、本発明の非接触ICカードにおける前記固定カードID生成手段は、書換え不可能なROM(リードオンリーメモリ)に記載された内容に基づき生成する構成とした。

【0013】

また、本発明の非接触ICカードにおける前記固定カードID生成手段は、書換え可能な不揮発メモリに記載された内容に基づき生成する構成とした。

【0014】

また、本発明の非接触ICカードにおける前記書換え可能な不揮発メモリは、EEPROM(Electrically Erasable Programmable Read Only Memory)、FeRAM(Ferroelectric Random Access Memory)、MRAM(Magnetoresistive Random Access Memory)、OUM(Ovonic Unified memory)のいずれかであることを特徴とする。

【0015】

また、本発明の前記リーダーライターと前記非接触ICカード間の通信方式はISO/IEC14443であり、カードIDは、前記リーダーライターから前記非接触ICカードに対する初期要求リクエストに対応したレスポンスにおけるPUPID(Pseudo-Unique PICC Identifier)として設定されることを特徴とする。

【0016】

また、本発明のカードID生成プログラムは、リーダライタと所定の方式により非接触通信を行う、非接触ICカードにおいて、該カードに備えるCPUにより実行される制御プログラムであって、前記非接触ICカードは、電源投入後、前記リーダライタから初めてカードIDの読み出し要求を受けた場合、乱数によりカードIDを生成し、該カードIDをリーダライタに通知するとともに、該カードIDを記憶し、電源投入後2回目以降に、前記リーダライタからカードIDの読み出し要求を受けた場合、記憶されたカードIDを読み出し、該カードIDをリーダライタに通知することを特徴とする。

【0017】

また、本発明の非接触ICカードのカードID生成集積回路は、リーダライタと所定の方式により非接触通信を行う、非接触ICカードの集積回路であって、乱数によりカードIDを生成する乱数カードID生成手段と、乱数カードID生成手段により生成されたカードIDを記憶するカードID記憶手段と、カードID読み出しが初回か否かを判定する初回判定手段と、カードIDの読み出し処理を行うカードID読み出し手段とを備え、電源投入後、前記リーダライタから初めてカードIDの読み出し要求を受けた場合、前記乱数カードID生成手段によりカードIDを生成し、該カードIDを出力することで、リーダライタに通知するとともに、該カードIDを前記カードID記憶手段に記憶し、電源投入後2回目以降に、前記リーダライタからカードIDの読み出し要求を受けた場合、前記カードID記憶手段に記憶されたカードIDを読み出し、該カードIDを出力することで、リーダライタに通知することを特徴とする。

【発明の効果】

【0018】

以上の構成により、本発明に係る非接触ICカードでは、初回のカードIDの読み出しには、カードIDに一意性がなく、それにより、個人の特定ができなくなる。また、2回目以降のカードIDの読み出しには、カードIDに一意性があり、それにより、リーダライタは特定のカードIDの非接触ICカードとの通信が可能となる。

【0019】

また、本発明に係る非接触ICカードでは、一度非接触ICカードとの通信が終了すると、リーダライタにとってはそのカードは別のカードと見なせるため、非接触ICカードが自身のカードIDを変更することが可能である。これにより、さらに個人の特定を不可とすることができる。

【0020】

また、本発明に係る非接触ICカードでは、カードIDの固定値の部分には、カードの発行者のIDや、サービスの種別などを記載することができ、乱数の部分に本発明が適応されるため、リーダライタは固定値の部分のカードIDをチェックすることでカードの情報を取得できると共に、個人の特定を不可とすることができる。

【0021】

また、本発明に係る非接触ICカードでは、モードに応じたカードIDの生成方法を非接触ICカードにおいて選択することが可能となる。その結果、プライバシーを気にしない場合、固定のカードIDを生成するモードでは、その固定のカードIDを用いることで特別なサービスを受けることが可能となり、逆にプライバシーを気にする場合、乱数のカードIDを生成するモードに変更を行うことにより、カード利用者の利便性の向上を図ることが可能である。

【0022】

また、本発明に係る非接触ICカードでは、ハードウェアの検査において、非接触の通信を用いてテスト可能な環境において、検査機が固定のカードIDを用いることが可能で、カードが応答するカードIDをパターンとして保持しておくことが可能で、カードIDに対応する計算を行う必要がなく検査の効率が向上する。一方、運用時にはカードIDは、乱数を用いることにより、個人のプライバシーを保護することが可能となる。

【0023】

また、本発明に係る非接触ICカードでは、前記検査機などでは、テストパターンを事

前に用意することが可能である。

【0024】

また、本発明に係る非接触ICカードでは、不揮発メモリに記載されているため、固定のカードID部分を書き換えることが可能となり、各種サービスに応じたカードIDを選択し、その値を書換え可能な不揮発メモリに格納することにより、プライバシーの向上をより図ることが可能となる。

【発明を実施するための最良の形態】

【0025】

以下本発明の実施の形態について、図面を参照しながら説明する。以下、本発明を近接型非接触ICカードの国際規格ISO/IEC14443に適應した場合の実施例を説明する。

ISO/IEC14443は、例えば、公共交通機関の改札ゲートなどで適用される通信規約のひとつである。より具体的には、図1に示すように、改札ゲートとして機能するリーダライタ100に乗車券カードとしての機能を有する非接触ICカード200及び非接触ICカード300を同時に差し込んだ場合を想定する。ISO/IEC14443の非接触ICカードの認識システムにおいては、以下の手順で非接触ICカードの認識が行われる。

【0026】

まず、改札ゲートであるリーダライタ100から初期要求リクエストを送信する。初期要求リクエストは、図2に図示されるフォーマットになっており、初期要求リクエストのPARAMのbit1～bit3の3bitにおいてタイムスロット数(N)を非接触ICカードに通知する。非接触ICカードは1～Nまでのスロットで応答する。今回の説明ではタイムスロット数(N)を4として説明を行なう。すなわち、初期要求リクエストに対して各非接触ICカード200及び300は、1～4までのタイムスロットのうち一つを選択し、初期応答を行う。

初期応答レスポンスは、図3に示されるフォーマットになっており、カードを識別するためのカードID(PUPI)、カードに搭載されているアプリケーション固有情報を通知するためのAPP Data、及び、リーダライタ100とのプロトコル情報を通知するためのProtocol Infを設定してリーダライタ100に応答を行う。各非接触ICカード200及び300からの初期応答レスポンスを受け取ったリーダライタ100は、受信した初期応答レスポンスのCRCの値等を参照し、衝突発生の有無を判定する。

【0027】

図4の一回目のカード識別処理において、リーダライタ100から初期要求リクエスト(「R1」で図示される)を送信する。初期要求リクエストに対して非接触ICカード200及び非接触ICカード300が、タイムスロット1(「A21」、「A31」で図示)でそれぞれ応答する。この場合、同一のタイミングで初期応答を応答するため、リーダライタ100は、非接触ICカードの衝突を検出する。したがって、再度、識別処理を再開する。

二回目の識別処理において、リーダライタ100から初期要求リクエスト(「R2」で図示)を送信する。初期要求リクエストに対して非接触ICカード200及び非接触ICカード300が、タイムスロット3(「A22」で図示)、およびタイムスロット2(「A32」で図示)で応答する。この場合、リーダライタ100は衝突を検出しないため、すべての非接触ICカードの識別を行なうことができ、識別処理を完了する。

【0028】

(実施の形態1)

図5は、本発明の実施の形態1にかかるリーダライタ100及び非接触ICカード200の構成を示す図である。リーダライタ100は、アンテナ101、送受信回路102、中央演算処理装置であるCPU103、リーダライタを制御するためのプログラムや、プログラム実行時に使用されるメモリ204により構成されている。メモリ204は、書換

え可能な不揮発メモリや、書き換え不可能なプログラムやデータを格納するROMや、プログラム実行時に一時的な作業領域として使用されるRAM等により構成されている。

非接触ICカード200は、アンテナ201、送受信回路202、中央演算処理装置であるCPU203、リーダーライタ100からのコマンドを処理するための制御プログラムや、プログラム実行時に使用されるメモリ204により構成されている。メモリ204は、書き換え可能な不揮発メモリや、書き換え不可能なプログラムやデータを格納するROMや、プログラム実行時に一時的な作業領域として使用されるRAM等により構成されている。

【0029】

さらに、本発明の特徴となる処理はROM205とRAM206により実現される。ROM205には乱数によりカードIDを生成する乱数カードID生成手段210、前記乱数カードID生成手段210によって生成されたカードIDを記憶するカードID記憶手段211、カードIDの読み出しが最初か否かを判定する初回判定手段212、及び、カードIDの読み出し処理を行うカードID読み出し手段213の制御プログラムをその中に備える。

ここで、乱数カードID生成手段210における乱数生成は、ソフトウェアによる擬似的な乱数手段の説明を行っているが、専用のハードウェアによる構成でも当然可能である。

また、RAM206には、カードID記憶手段211で記憶されるカードID記憶領域、及び、初回判定手段212の判定用に用いる初回判定フラグ（図示せず）を記憶する。この初回判定フラグは、非接触ICカードの電源投入時に初期化（例えば0に設定）されるRAM206内の変数で、初回判定フラグが0の場合、初回読み出しを意味し、0以外の場合、2回目以降の呼び出しを意味する。

【0030】

図6は、非接触ICカード200におけるカードID生成方法のフローチャートである。

まず、最初にカードIDの読み出し処理が最初に呼び出された場合の説明を行う。非接触ICカード200は、カードID読み出し処理が最初に呼ばれているか否かを保持する初回判定フラグを読み出す（ステップS201）。

続いて読み出しを行った初回判定フラグの値を判定する（ステップS202）。前記記載の通り、初回のカードID読み出し処理では、初回判定フラグの値が0であるので、カードIDを生成するためにカードID生成処理（ステップS203）へ制御を移す。

続いて、カードIDを生成するため、乱数カードID生成手段210によりカードIDを生成する（ステップS203）。

続いて、上記生成されたカードIDを、カードID記憶領域に保存する（ステップS204）。

さらに、これ以後のカードIDの変更を行ってはならないので、初回判定フラグの値に1を設定する（ステップS205）。

最後に、カードID記憶領域に保存したカードIDを読み出し（ステップS206）処理を終了する。

【0031】

続いて、二回目以降のカードIDの読み出し処理の説明を行う。一回目と同様に、非接触ICカード200は、カードID読み出し処理が最初に呼ばれているか否かを保持する初回判定フラグを読み出す（ステップS201）。

続いて、読み出しを行った初回判定フラグの値を判定する（ステップS202）。前記記載の通り、二回目以降のカードID読み出し処理では、初回判定フラグの値が1であるので、保存されているカードIDを読み出すため（ステップS206）へ制御を移す。

最後に、カードID記憶領域に保存したカードIDを読み出し（ステップS206）処理を終了する。

【0032】

以上のような処理を行うことにより、初回のカードIDの読み出しでは、カードIDに一意性がなく、個人の特定ができなくなる。また、二回目以降のカードIDの読み出しには、カードIDに一意性があり、それにより、リーダライタはカードを特定した通信が可能となる。

【0033】

(実施の形態2)

図7は、本発明の実施の形態2にかかる非接触ICカード200の構成を示す図である。

非接触ICカード200は、アンテナ201、送受信回路202、中央演算処理装置であるCPU203、リーダライタ100からのコマンドを処理するための制御プログラムや、プログラム実行時に使用されるメモリ204により構成されている。メモリ204は、書換え可能な不揮発メモリや、書き換え不可能なプログラムやデータを格納するROMや、プログラム実行時に一時的な作業領域として使用されるRAM等により構成されている。

【0034】

さらに、本発明の特徴となる処理はROM205とRAM206により実現される。ROM205にはカードIDの読み出しが最初か否かを判定する初回判定手段212、カードIDの読み出し処理を行うカードID読み出し手段213、及び、動作モードを判定するモード判定手段215を備える。前記モード判定手段215は、乱数IDモードと固定IDモードの2つのモードを持ち、乱数IDモードの場合は乱数カードID生成手段210を用いてカードIDを生成し、固定IDモードの場合は固定カードID生成手段214を用いてカードIDを生成する。生成されたカードIDは、カードID記憶手段211に記憶する。

RAM206には、カードID記憶手段211で記憶されるカードID記憶領域、及び、初回判定手段212の判定用に用いる初回判定フラグ(図示せず)を記憶する。

この初回判定フラグは、非接触ICカードの電源投入時に初期化(例えば0に設定)されるRAM206内の変数で、初回判定フラグが0の場合、初回読み出しを意味し、0以外の場合、2回目以降の呼び出しを意味する。

【0035】

図8は、非接触ICカード200におけるカードID生成方法のフローチャートである。

まず、最初にカードIDの読み出し処理が最初に呼び出された場合の説明を行う。非接触ICカード200は、カードID読み出し処理が最初に呼ばれているか否かを保持する初回判定フラグを読み出す(ステップS301)。

続いて読み出しを行った初回判定フラグの値を判定する(ステップS302)。前記記載の通り、初回のカードID読み出し処理では、初回判定フラグの値が0であるので、カードIDを生成するためにカードID生成処理(ステップS303)へ制御を移す。

続いてカードIDの生成の種別を判定するためモードフラグの読み出しを行い、モードの判定を行う(ステップS303、ステップS304)。判定したモードが乱数のIDを生成するモードの場合、乱数カードID生成手段210によりカードIDを生成する(ステップS305)。判定したモードが固定のIDを生成するモードの場合、固定カードID生成手段214によりカードIDを生成する(ステップS306)。

続いて、上記生成されたカードIDを、カードID記憶領域に保存する(ステップS307)。さらに、これ以後のカードIDの変更を行ってはならないので、初回判定フラグの値に1を設定する(ステップS308)。最後に、カードID記憶領域に保存したカードIDを読み出し(ステップS309)処理を終了する。

【0036】

続いて、二回目以降のカードIDの読み出し処理の説明を行う。一回目と同様に、非接触ICカード200は、カードID読み出し処理が最初に呼ばれているか否かを保持する初回判定フラグを読み出す(ステップS301)。

続いて、読み出しを行った初回判定フラグの値を判定する(ステップS302)。前記記載の通り、二回目以降のカードID読み出し処理では、初回判定フラグの値が1であるので、保存されているカードIDを読み出すため(ステップS309)へ制御を移す。最後に、カードID記憶領域に保存したカードIDを読み出し(ステップS309)処理を終了する。

【0037】

以上のような処理を行うことにより、モードに応じたカードIDの生成方法を非接触ICカードにおいて選択することが可能となる。これにより、プライバシーを気にしない場合、固定のカードIDを生成するモードでは、その固定のカードIDを用いることで特別なサービスを受けることが可能となり、逆にプライバシーを気にする場合、乱数のカードIDを生成するモードに変更を行うことにより、カード利用者の利便性の向上を図ることが可能である。

また固定のモードが、ハードウェアの検査の場合、検査機が固定のカードIDを用いることが可能で、カードが応答するカードIDをパターンとして保持しておくことが可能となり、カードIDに対応する計算を行う必要がなく検査の効率が向上する。一方、運用時にはカードIDは、乱数を用いることにより、個人のプライバシーを保護することが可能となる。

さらに、固定のカードIDが書換え不可なROM(リードオンリーメモリ)に記載されている場合、前記検査機などでは、テストパターンを事前に用意することが可能である。

【0038】

さらに、固定のカードIDが、書換え可能な不揮発メモリに記載されている場合、固定のカードID部分を書き換えることが可能となる。

なお、書換え可能な不揮発メモリとは、具体的に、EEPROM(Electrically Erasable Programmable Read Only Memory)、FeRAM(Ferroelectric Random Access Memory)、MRAM(Magnetoresistive Random Access Memory)、OUM(Ovonic Unified memory)である。

【0039】

(実施の形態3)

図9は、本発明の実施の形態3にかかる非接触ICカード200の構成を示す図である。非接触ICカード200は、アンテナ201、送受信回路202、中央演算処理装置であるCPU203、リーダライタ100からのコマンドを処理するための制御プログラムや、プログラム実行時に使用されるメモリ204により構成されている。メモリ204は、書換え可能な不揮発メモリや、書き換え不可能なプログラムやデータを格納するROMや、プログラム実行時に一時的な作業領域として使用されるRAM等により構成されている。

【0040】

さらに、本発明の特徴となる処理はROM205とRAM206により実現される。ROM205には乱数によりカードIDを生成す乱数カードID生成手段210、前記カードID生成手段210によって生成されたカードIDを記憶するカードID記憶手段211、カードIDの読み出しが最初か否かを判定する初回判定手段212、カードIDの読み出し処理を行うカードID読み出し手段213、及び、通信終了判定手段216の制御プログラムをその中に備える。

また、RAM206には、カードID記憶手段211で記憶されるカードID記憶領域、及び、初回判定手段212の判定用に用いる初回判定フラグ(図示せず)を記憶する。

この初回判定フラグは、非接触ICカードの電源投入時に初期化(例えば0に設定)されるRAM206内の変数で、初回判定フラグが0の場合、初回読み出しを意味し、0以外の場合、二回目以降の呼び出しを意味する。

【0041】

ここで、通信終了判定手段216の処理を説明する。

通信終了判定手段216は、通信の終了を監視し通信の終了が判定された場合、前記の初回判定フラグの値を0に変更する。通信の終了が判定されない場合には、初回判定フラグに対して何も値を設定しない。

実施の形態1及び、実施の形態2で明らかなように、この初回判定フラグの値を0にした場合、新規にカードIDを生成する。したがって、通信が終了した場合、次のカードID読み出し処理が行われると新規にカードIDを生成する。

以上のように、一度非接触ICカードとの通信が終了すると、リーダライタにとってはそのカードは別のカードと見なせるため、非接触ICカードが自身のカードIDを変更することが可能である。これにより、さらに個人の特定を不可とすることができる。

【0042】

(実施の形態4)

これまで、カードIDは、乱数値もしくは、固定値であるような例を説明したが、カードIDが乱数により構成される部分と、固定値により構成される部分の両方を含む場合がある。カードIDが複数のリーダライタ間で特定されなければ、本発明の目的を達しているので、カードIDの一部を固定値としてよい。

本発明に係る非接触ICカードでは、カードIDの固定値の部分には、カードの発行者のIDや、サービスの種別などを記載することができ、乱数の部分に本発明が適応されるため、リーダライタは固定値の部分のカードIDをチェックすることでカードの情報を取得できると共に、個人の特定を不可とすることができる。

この場合、乱数により構成される部分は乱数カードID生成手段210により生成され、固定値により構成される部分は固定カードID生成手段214により生成される。

【0043】

(実施の形態1～実施の形態4の補足事項1)

以上、実施形態1、2、3、4を説明した。尚、これまでの説明において本発明の非接触ICカードにおいて備えている、乱数カードID生成手段、カードID記憶手段、初回判定手段、カードID読み出し手段、通信終了判定手段、モード判定手段、固定カードID生成手段等の各機能ブロックは典型的には、コンピュータプログラムとして実現される。当該プログラムは、非接触ICカード内のROMに格納され実行されるものと、外部よりダウンロードされ、不揮発性メモリに格納され実行されるものがある。

【0044】

(実施の形態1～実施の形態4の補足事項2)

また、さらに、上述の機能ブロックは、CPU、RAM、ROM、不揮発性メモリ等のハードウェア資源との組み合わせにより、集積回路であるLSIとして実現される場合がある。これらは、個別に1チップ化されても良いし、一部又はすべてを含むように1チップ化されても良い。

図10、図11、図12に実施の形態1、実施の形態2、実施の形態3における集積回路化の一例を示す。LSI1001、LSI1002、LSI1003は集積回路化の一例を示し、集積回路化する機能ブロックの範囲の例である。

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製作後にプログラムすることが可能なFPGA(Field Programmable Gate Array)やLSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【産業上の利用可能性】

【0045】

本発明にかかる非接触ICカードにおけるカードID生成方法は、カードIDに一意性

をなくし、カード使用者のプライバシーを保護するのみでなく、リーダライタが特定の非接触 I C カードとの通信も可能となるため、非接触の通信が行われるシステム(R F タグ等)の用途にも応答が可能である。

【図面の簡単な説明】

【0046】

【図1】本発明のシステムの使用形態例を示す図

【図2】本発明の実施の形態1における初期要求リクエストのフレーム図

【図3】本発明の実施の形態1における初期応答のフレーム図

【図4】本発明の実施の形態1におけるリーダライタと非接触 I C カードのカード検索処理を示す図

【図5】本発明の実施の形態1におけるリーダライタと非接触 I C カードのモジュール構成図

【図6】本発明の実施の形態1における非接触 I C カードのフローチャート図

【図7】本発明の実施の形態2における非接触 I C カードのモジュール構成図

【図8】本発明の実施の形態2における非接触 I C カードのフローチャート図

【図9】本発明の実施の形態3における非接触 I C カードのモジュール構成図

【図10】本発明の実施の形態1における非接触 I C カードにおいて、LSIを備えた場合のモジュール構成図

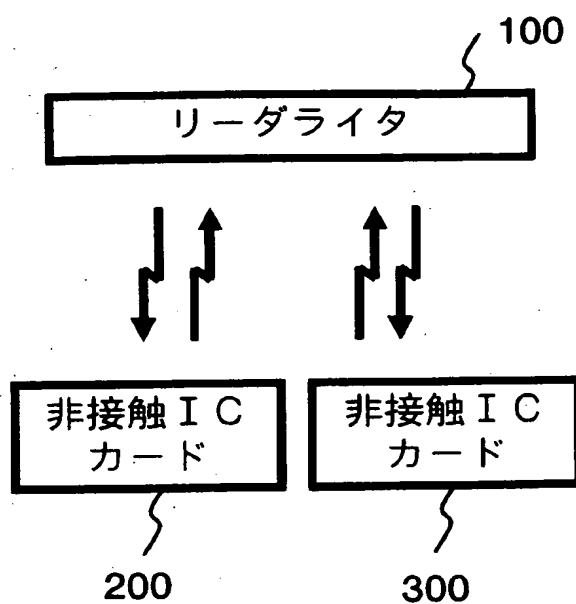
【図11】本発明の実施の形態2における非接触 I C カードにおいて、LSIを備えた場合のモジュール構成図

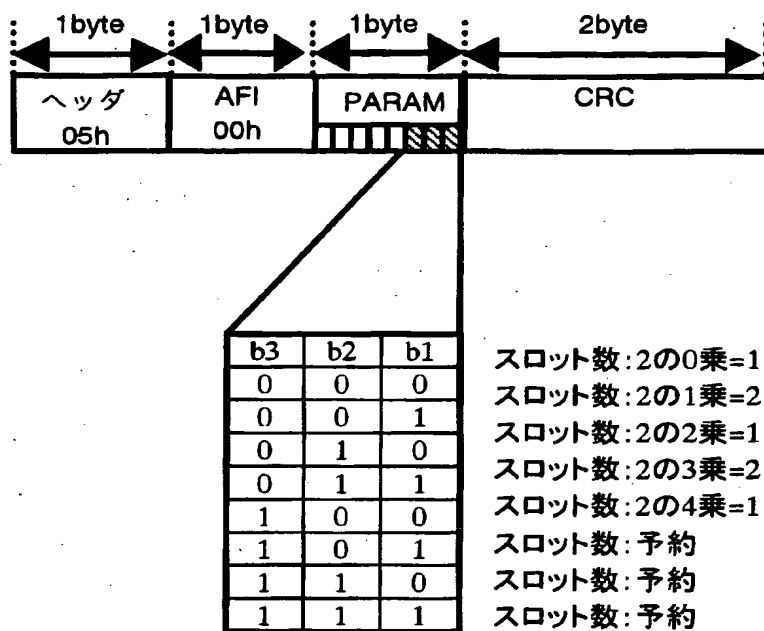
【図12】本発明の実施の形態3における非接触 I C カードにおいて、LSIを備えた場合のモジュール構成図

【符号の説明】

【0047】

- 100 リーダライタ
- 101 アンテナ
- 102 送受信回路
- 103 CPU
- 104 メモリ(RAM/ROM/不揮発性メモリ)
- 200 非接触 I C カード
- 201 アンテナ
- 202 送受信回路
- 203 CPU
- 204 メモリ(RAM/ROM/不揮発性メモリ)
- 205 ROM
- 206 RAM
- 210 乱数カード I D 生成手段
- 211 カード I D 記憶手段
- 212 初回判定手段
- 213 カード I D 読出手段
- 214 固定カード I D 生成手段
- 215 モード判定手段
- 216 通信終了判定手段
- 300 非接触 I C カード
- 1001 LSI
- 1002 LSI
- 1003 LSI



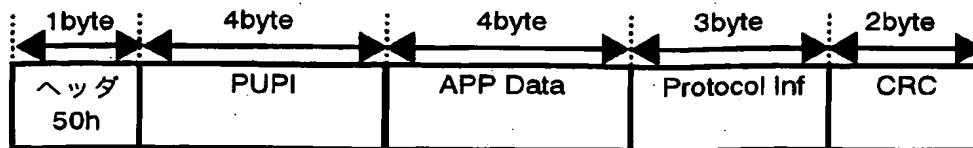


ヘッダ : 初期要求コマンド

AFI : 非接触 I C カードの適応クラス (全クラス)

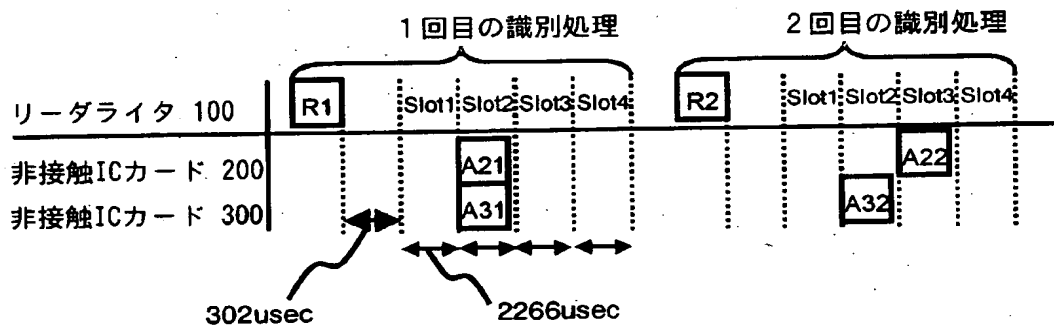
CRC : AP~PARAMまでのCRC値

【図 3】



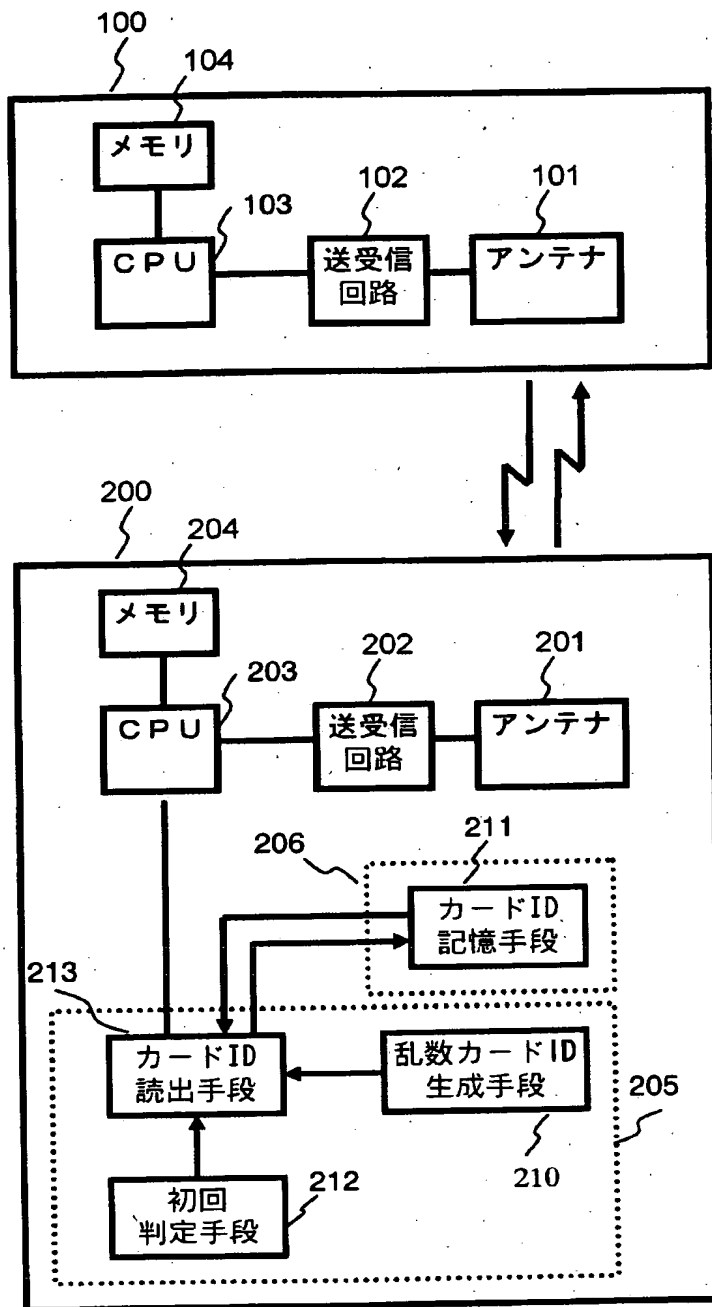
ヘッダ : 初期応答ヘッダ
 PUI : カードID(Pseudo-Unique PICC Identifier)
 App Data : アプリケーション固有情報
 Protocol Inf : プロトコル情報
 CRC : ヘッダ～Protocol InfまでのCRC値

【図 4】

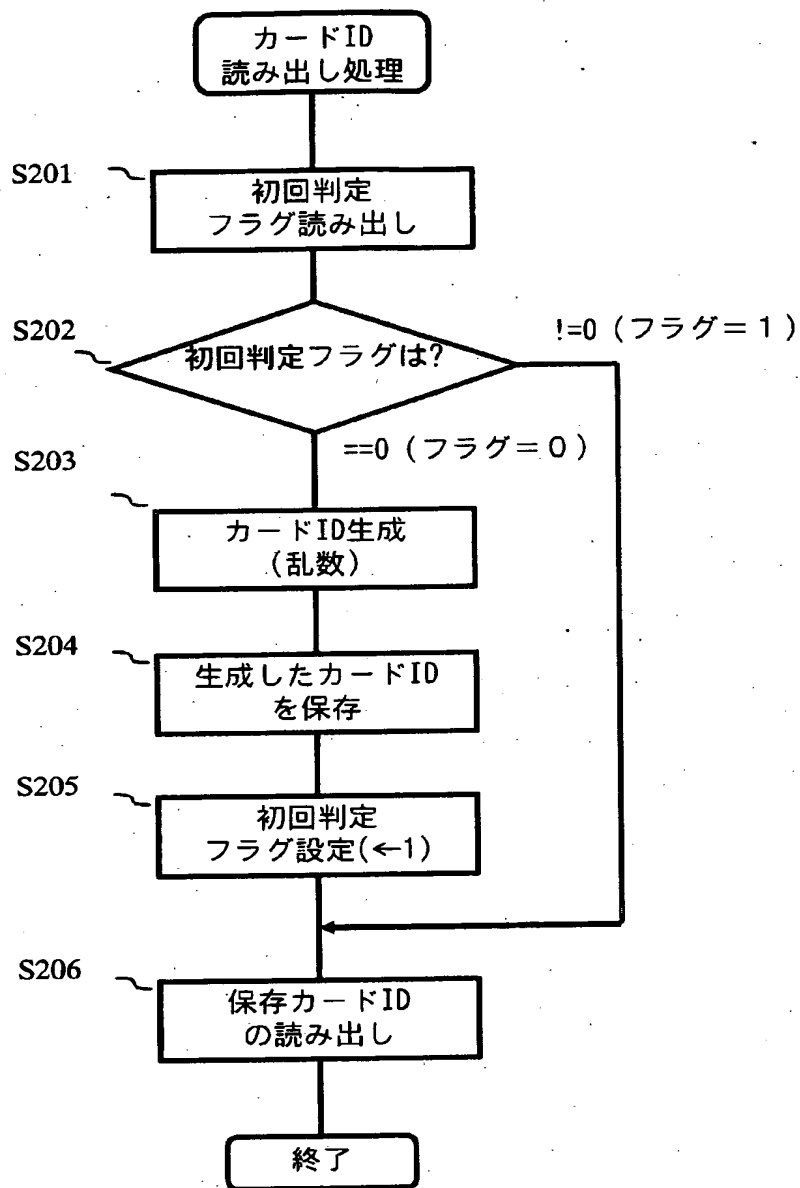


R1, R2 : 初期要求リクエスト[REQB] (リーダライタから非接触ICカード)
 A21, A22 : 初期応答[ATQB] (非接触ICカード200からリーダライタ100)
 A31, A32 : 初期応答[ATQB] (非接触ICカード300からリーダライタ100)
 Slot1~Slot4 : タイムスロット番号

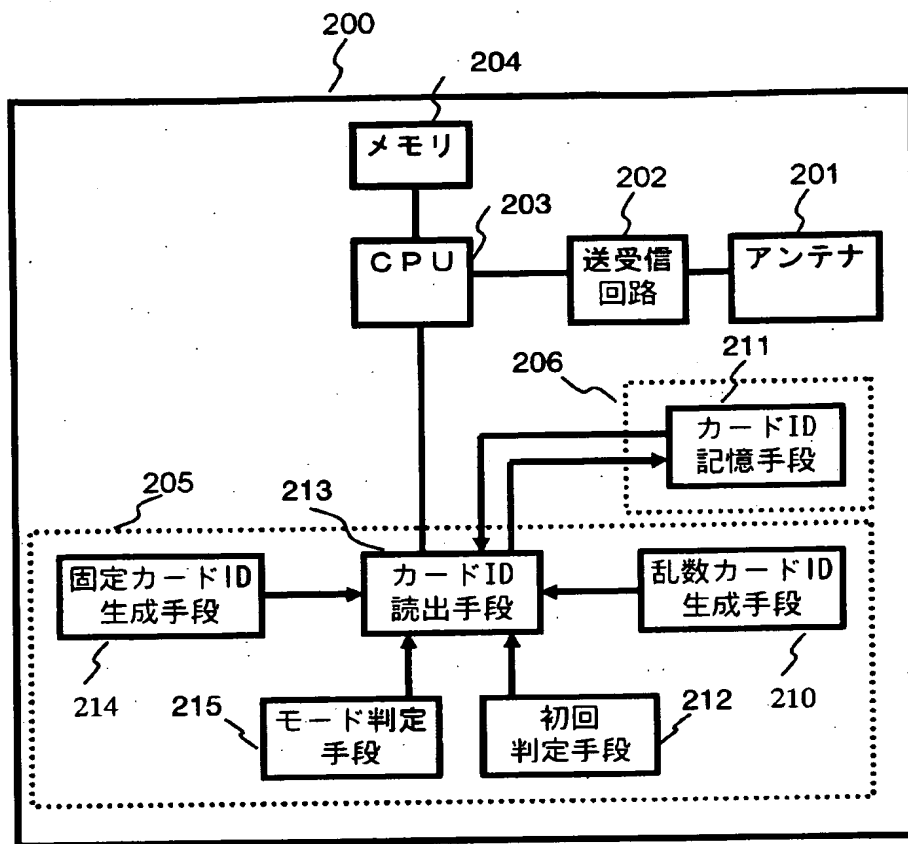
【図5】



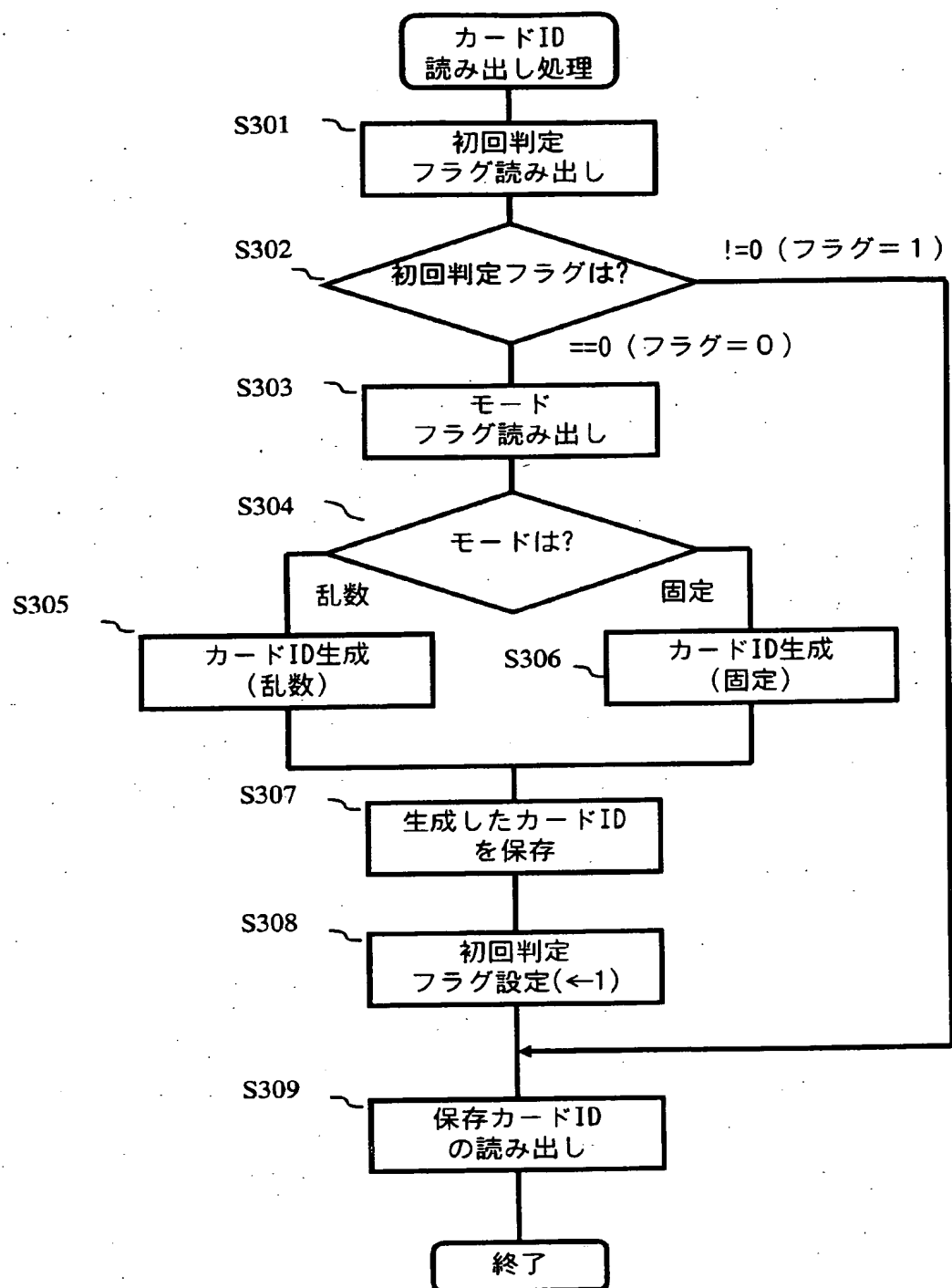
【図6】



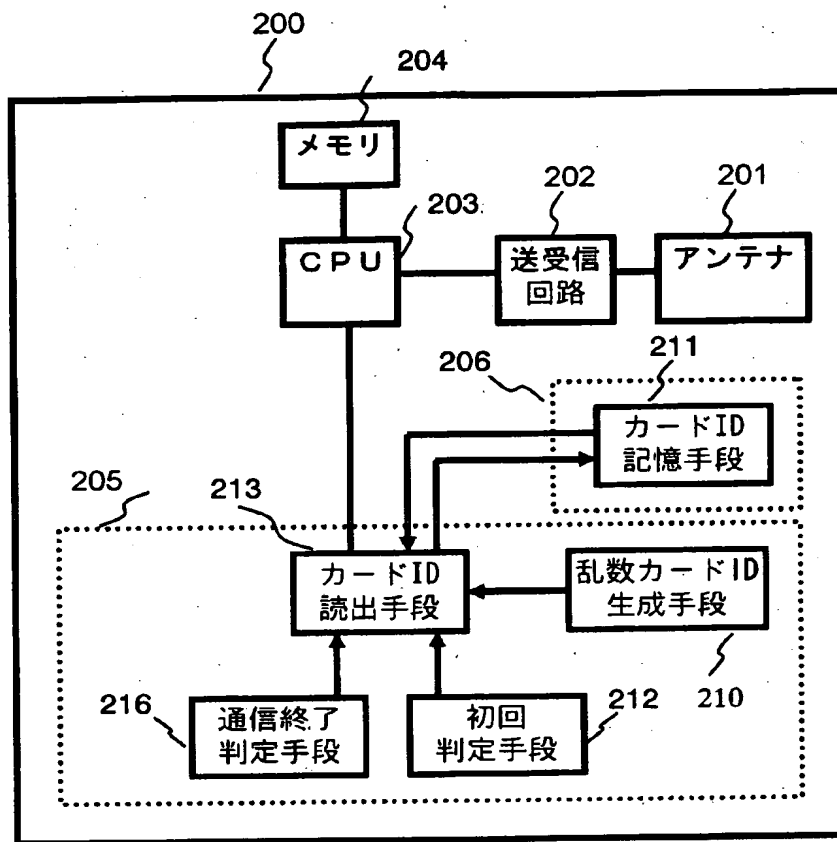
【図 7】

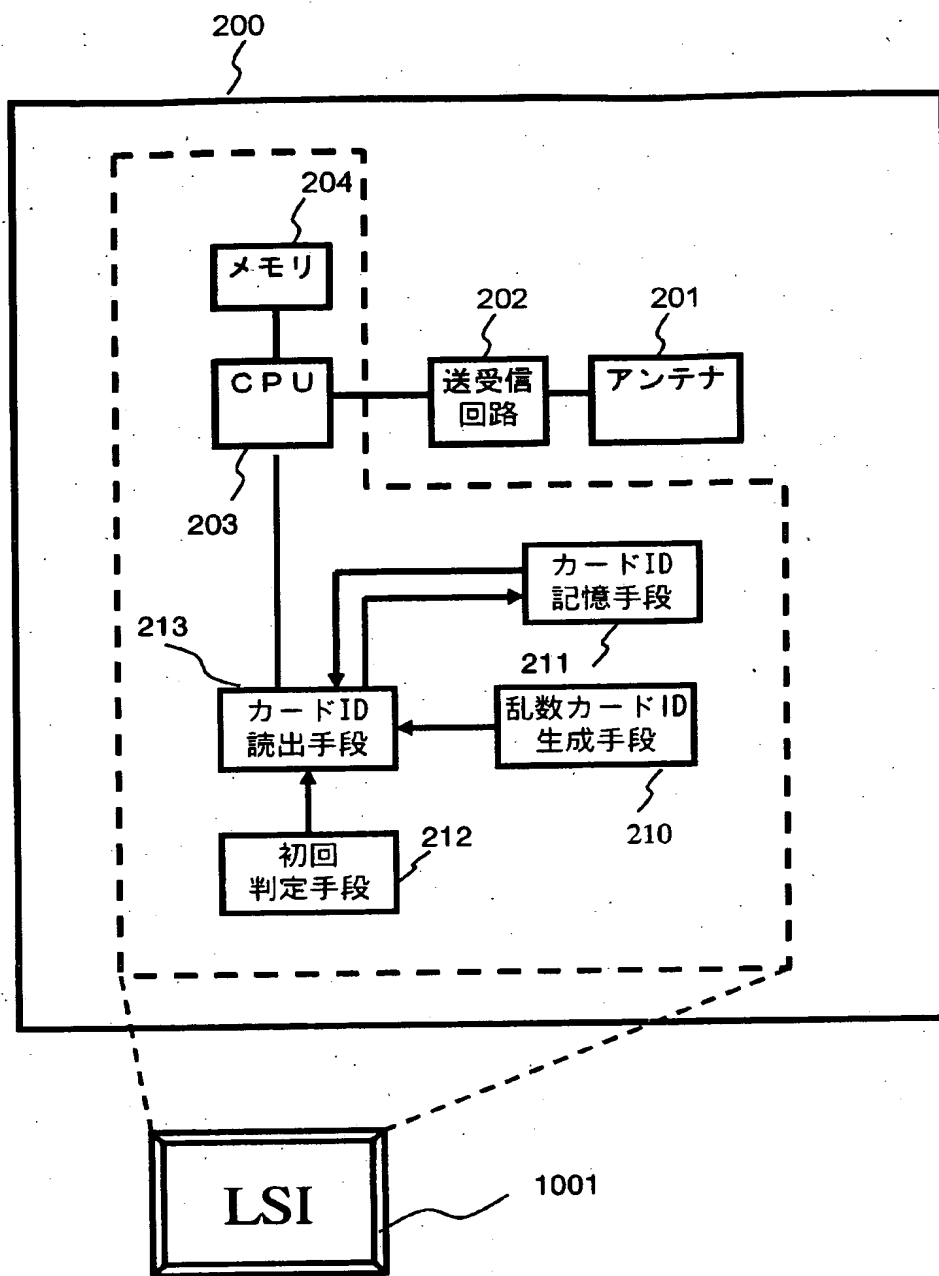


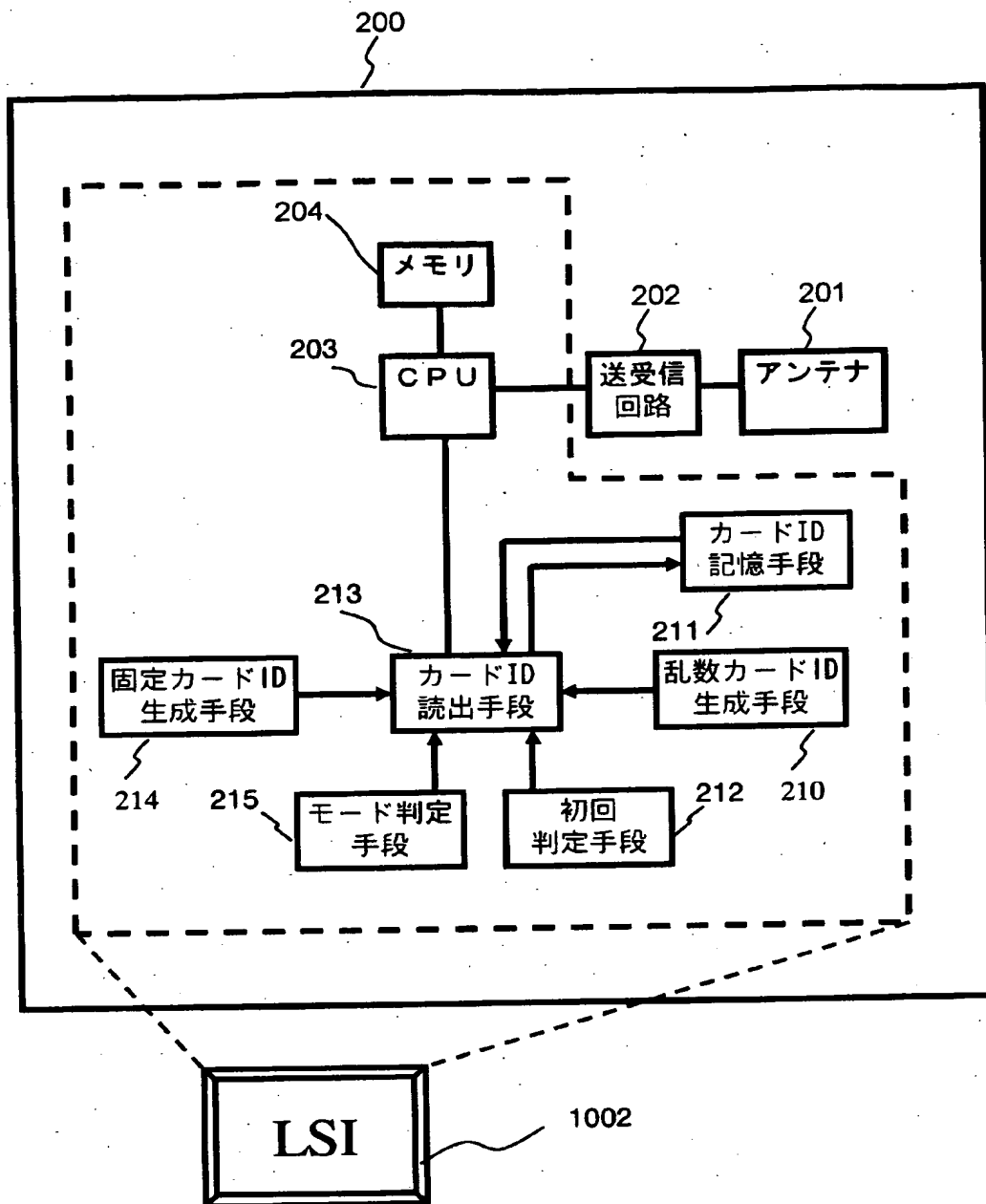
【図 8】

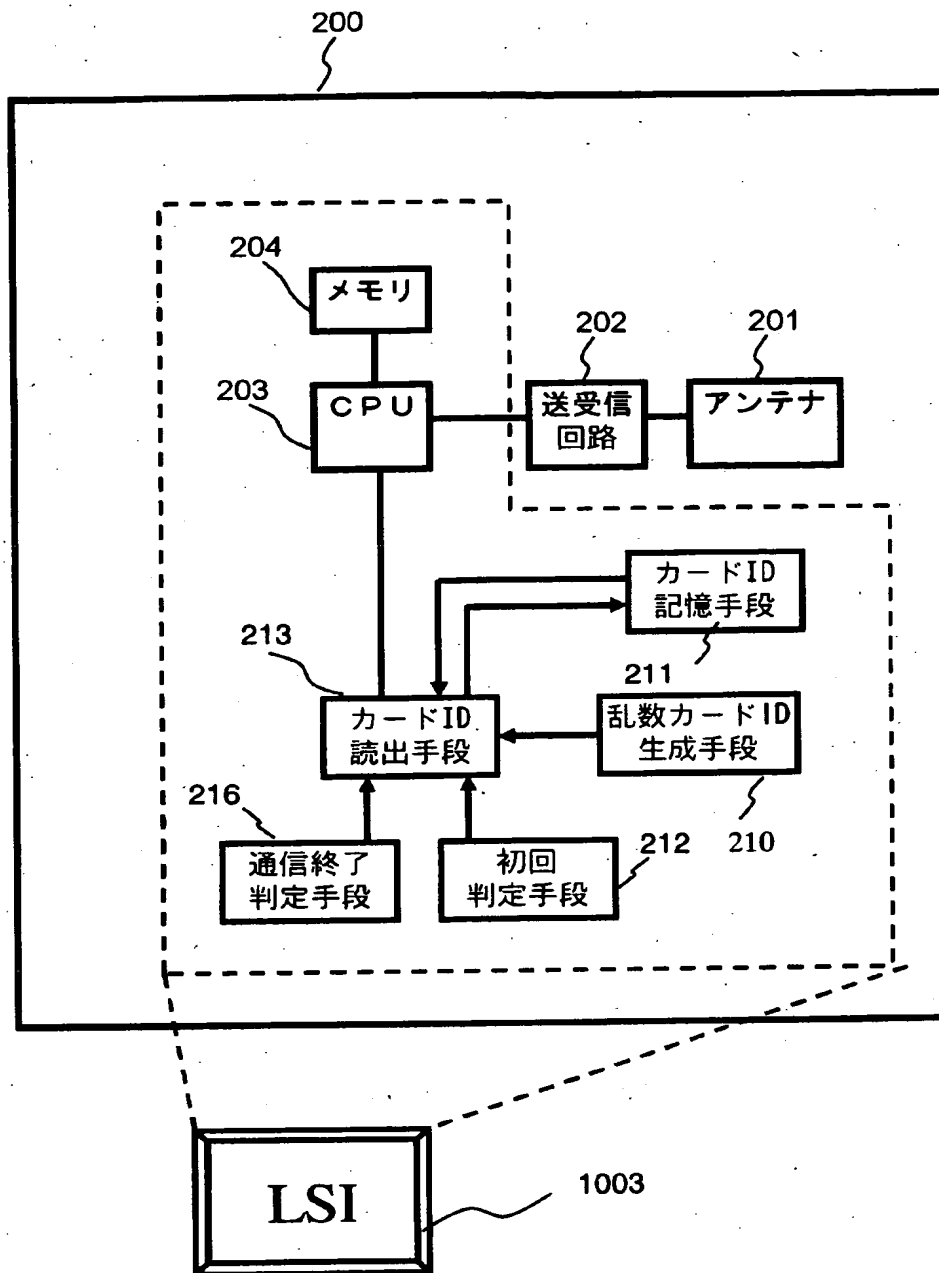


【図 9】









From the INTERNATIONAL BUREAU

PCTNOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

NII, Hiromori
c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center
Bldg., 11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi
Osaka 5320011
JAPON

| | |
|---|--|
| Date of mailing (day/month/year) 24 June 2005 (24.06.2005) | |
| Applicant's or agent's file reference P37577-P0 | IMPORTANT NOTIFICATION |
| International application No. PCT/JP05/007194 | International filing date (day/month/year) 07 April 2005 (07.04.2005) |
| International publication date (day/month/year) | Priority date (day/month/year) 14 April 2004 (14.04.2004) |
| Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al | |

- By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- (If applicable)* The letters "NR" appearing in the right-hand column denote a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- (If applicable)* An asterisk (*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b) (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

| <u>Priority date</u> | <u>Priority application No.</u> | <u>Country or regional Office or PCT receiving Office</u> | <u>Date of receipt of priority document</u> |
|----------------------------|---------------------------------|---|---|
| 14 April 2004 (14.04.2004) | 2004-118807 | JP | 20 May 2005 (20.05.2005) |

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 740 14 35

Authorized officer

Hennequin Françoise

Facsimile No. +41 22 338 70 10
Telephone No. +41 22 338 9935

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

NII, Hiromori
c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center
Bldg., 11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi
Osaka 5320011
JAPON

| | |
|---|--|
| Date of mailing (day/month/year) 24 June 2005 (24.06.2005) | |
| Applicant's or agent's file reference P37577-P0 | IMPORTANT NOTIFICATION |
| International application No. PCT/JP05/007194 | International filing date (day/month/year) 07 April 2005 (07.04.2005) |
| International publication date (day/month/year) | Priority date (day/month/year) 14 April 2004 (14.04.2004) |
| Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al | |

- By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- (If applicable)* The letters "NR" appearing in the right-hand column denote a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- (If applicable)* An asterisk (*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b) (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

| <u>Priority date</u> | <u>Priority application No.</u> | <u>Country or regional Office or PCT receiving Office</u> | <u>Date of receipt of priority document</u> |
|----------------------------|---------------------------------|---|---|
| 14 April 2004 (14.04.2004) | 2004-118807 | JP | 20 May 2005 (20.05.2005) |

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 740 14 35

Authorized officer

Hennequin Francoise

Facsimile No. +41 22 338 70 10
Telephone No. +41 22 338 9935